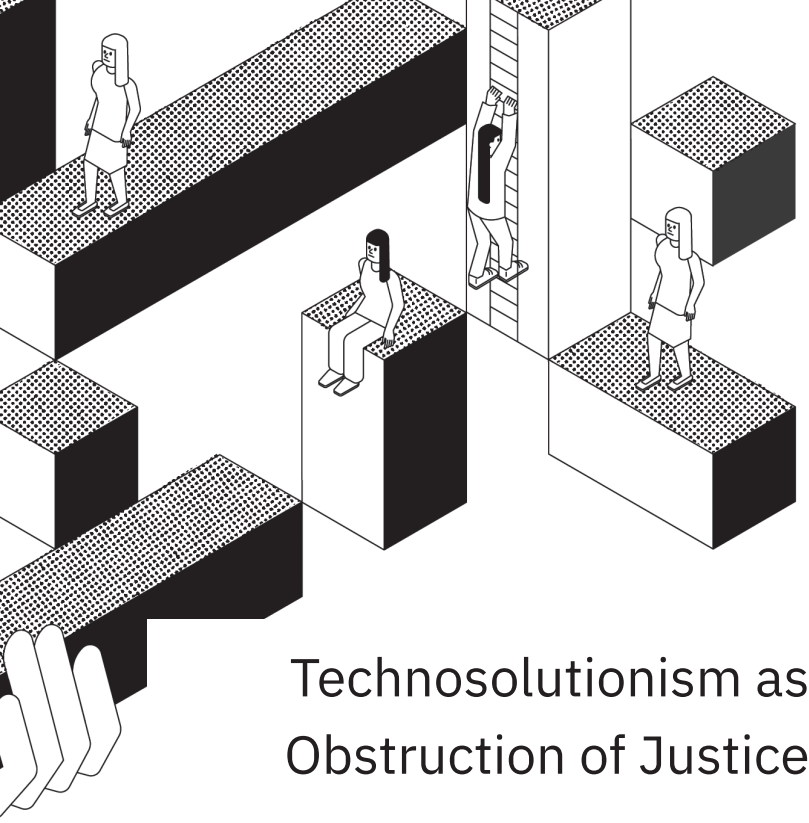


# Technosolutionism as Obstruction of Justice

**ALEXANDRA ARGÜELLES**

Alex Argüelles is a technologist with a degree in communication science, a member of Ciberseguras and founder of the **comun.al** digital resilience laboratory. Since 2013, they have collaborated on human rights and technological initiatives in Latin America, engaging in advocacy and analysis with an emphasis on privacy, gender, accessibility and inclusion. They facilitate workshops and provide digital security support for the region's journalists and activists with a psychosocial focus and a transformative justice approach. They currently form part of the Mozilla Foundation's Technology and Society program, addressing the sociopolitical violence exercised through technologies in Mexico.

**WHEN WE CONFRONT** digital violence, the first thing that tends to come to mind is that we have to restore the security of our devices or accounts. We want to take back control of our information and even identify the origin of the attack or the violence to which we're being subjected. Once we have an idea of how to respond, we seek out mechanisms to report or denounce it and we demand justice for the aggressions we've experienced, but what does justice mean and how can we access it? Under what terms—or whose—do we define access to justice?

Justice has several meanings. We can think of it as a common good, as an indispensable condition for personal development, as the set of criteria that establish the limits of the relationships in which we participate (as individuals, as members of society, as political subjects, etc.) so that human rights are respected and conditions established that allow us to exercise them as broadly as possible. According to the political project of transformative justice, we can think of justice as a response to violence, harm and abuse that aims for restoration, healing and the transformation of both the people involved and their environments to prevent the spread of violence, ensuring shared responsibility and community resilience. In theory, the functions of the state—even in Mexico—include that of ensuring that justice is done through its authority over the territory and those who live in it.

Returning to the theme of digital violence, it's

interesting to see how an inconsistent discourse has arisen over the last ten years regarding the ways in which the state provides responses or "justice" in situations of violence propagated through technology while reinforcing its use as a way of consolidating capacities of control to improve the "security" that it offers. I put justice and security in quotes because these concepts have been so cheapened through the shortsighted arguments of those who rule us that they have become proof of the inability to understand and address the complexity that should characterize them.

In response to digital violence, particularly gender violence, specialized agencies have been founded and there have been legal reforms to expand the criminal code to include some manifestations of violence that utilize technology. As on many other fronts on which we defend dignity in the pursuit of justice, the struggle for the recognition of the effects of digital violence was led by people who had been victims of it and were revictimized by the state, which denied them justice, excusing itself with the negligent lack of a feminist perspective and the absence of the tools needed to meet its responsibilities that—like violence—have also moved to digital environments. In Mexico, raising consciousness and developing measures to respond to gender violence expressed through technologies is an achievement of those who organized to develop skills and share them with others who were going through

similar situations, as was the case with the activist Ana Baquedano, but it's also an achievement of those who used their legal and organizing skills to shape the development of reforms promoting the recognition of the seriousness of this violence, such as the Frente Nacional para la Sororidad and Defensoras Digitales and all their local chapters across the country.

There is also a more "industrial" vision of all this. Here, one doesn't speak of digital violence so much as "cybercrime." This can refer to anything from identity theft for the purpose of banking fraud to alleged copyright violations that, as we have often seen, beyond protecting the interests of creators or industries, have been used as an agile form of censorship and content removal by the state. Here is where the interests of the state and the many industries that have incorporated digital technologies often coincide in opposition to the public interest, obstructing the exercise of human rights.

In both cases, we see how responses have been developed to address harm within the current legal framework, but when we see the treatment given to the interests of civil society compared to those of industries or the state, the difference is clear. The recognition of digital violence and its effects has been a constant struggle by organized civil society (led by women and members of the LGBTIQ+ community), and this recognition of its seriousness—as a continuation of the macho, misogynistic, sexist violence that

we experience every day in physical environments—demands access to the justice we have been denied for so many years. Its nuances also involve questions in which the freedom of expression and the violence against journalists, activists and human rights defenders in Mexico intersect with questions of inequality and gaps in access to information, education, health or culture; at the same time, "cybercrime" has served to spark conversations on how the state has consolidated its capacity for control through political persecution, device hacking and mass surveillance under the pretext that the use of increasingly abusive technologies is the key to protecting us from potential cybercriminals. It has been said that a state that assumes that all the people it governs are potential criminals is a state that seeks to criminalize as a form of governing, ignoring the presumption of innocence: disciplining and punishing to control those who live as perpetual suspects rather than providing answers for situations of inequality or addressing different contexts in all their complexity, thus failing to ensure that justice is done.

The prefix cyber- thus allows for a new class of euphemisms that the state and its representatives—in the different branches of government—have skillfully instrumentalized to surveil, punish, persecute and criminalize through tools as powerful as they are sophisticated...monopolizing the "legitimate use of force" through technology as well. We have seen how these euphe-

misms demand special powers when used in discourses that promote state security strategies involving the implementation of technologies that directly affect fundamental rights, such as the right to privacy or even the freedom of expression or the right to information.

The use of these technologies, their abusive instrumentalization to consolidate power and the development of legislation that tends toward the development of policies that center their efficiency on this use are just some examples of how technosolutionism is manifested: a hyperbiased way of addressing complex problems that attempts to show a simplified correlation between the implementation of certain technologies and the effects desired in order to manage situations that the state has been unable to resolve.

We can find a clear example of this ambivalent approach to justice and technology in the 2013 consolidation of Internet access as a constitutional right in Mexico. The recognition of this right has to do with the possibilities that providing Internet access creates for other rights, such as the right to information and the freedom of expression, which are fundamental to the individual and collective development needed for democracy to be fully expressed and exercised. Nevertheless, the same reform that established this right in our country was accompanied by secondary legislation that benefited telecommunications monopolies (by weakening net neutral-

ity—a fundamental principle for ensuring free access to information without regard to its origins, platform or format—in order to benefit the market) and offered pathways to legitimizing abuses of state power through technologies, such as blocking telecommunications services or monitoring digital activities through real-time geolocation without the need for the prior authorization of a judge.

In April 2014, many of us took the streets to protest against this secondary legislation, demanding respect for net neutrality and our right to privacy as guarantees for the exercise of the freedom of expression and the right to information. In July of that year, a reform was approved of the Federal Telecommunications and Radio Broadcasting Law, whose Article 145 establishes that the Federal Telecommunications Institute (an autonomous government agency created one year earlier to regulate and supervise the country's digital networks, telecommunications services and radio stations) should issue a series of guidelines to ensure net neutrality, in accordance with the principles of free choice, non-discrimination, privacy, transparency and information, traffic management, quality and sustained infrastructure development. Article 146 of this law determined that "Concessionaires and authorized vendors must provide Internet service that respects the capacity, speed and quality contracted by the user, independently of content, origin, destination, terminal or application,

as well as of the services that are provided via the Internet, in compliance with the provisions of the previous article."

By January 2019, the Federal Telecommunications Institute had still not issued the guidelines that would guarantee net neutrality and those rights that had been affected by the lack of mechanisms for protecting privacy, access to information and the freedom of expression. In response, Red en Defensa de los Derechos Digitales sued for the institute to meet its obligation to issue these guidelines. This lawsuit was decided in favor of civil society and it was ruled that the institute must issue the pending guidelines by the second trimester of 2021 at the very latest. In December 2019, the Federal Telecommunications Institute released for public comment the draft guidelines on traffic management and network administration, which would have the following objectives:

i) To guarantee that the end user has the freedom to choose the contents, applications and services they use and an understanding of how the traffic on their network is managed.
ii) To provide legal certainty for the industry in terms of net neutrality through clarity on viable traffic management and network administration policies and respect for admissible commercial practices.

iii) To encourage innovation in the sector through the use of more efficient technologies in networks and new commercial strategies.
iv) To promote the reduction of the digital divide through commercial offers aligned with traffic management and network administration policies authorized by the institute for specific objectives.
v) To promote competitive conditions.
vi) To incentivize investment in networks to provide fixed and mobile Internet access with greater quality and coverage.

While it's clear at first glance that these objectives are in line with the interests of the telecommunications industry and its development, the document in which they were presented contained another vision entirely. The draft contained guidelines that gave the state the power to remove content, applications and Internet services, permitted Internet traffic to be monitored through deep packet inspection and for certain content to be prioritized to benefit the commercial partners of Internet service providers (directly interfering with access to information and even affecting fair competition with independent content producers and services), omitting the counterweights needed to ensure the protection of net neutrality.

In response to these guidelines that sought to favor the industry's interests by weakening our

rights, the campaign #SalvemosInternet[108] managed to convoke over 150,000 people across the country to participate in this public comment process, expressing concerns that have been present since 2014, as both the objectives and the proposed guidelines made clear that the primary interest behind this proposal wasn't the defense of net neutrality or our digital rights, but protecting the interests of private companies and consolidating the state's mechanisms of surveillance and control: precisely the same reasons we had taken the streets seven years beforehand.

The constitutional recognition of Internet access as a right seems to be an absolute victory in the consolidation of human rights as they are being broadened through technology—what we tend to call digital rights—but we also see how, in this victory, the interests of the prevailing actors—in this case, private companies and the government—enter into tension with this broadening of our rights. To avoid losing the power they have consolidated, we have seen how these prevailing actors end up developing opaque measures to reduce our rights that are not only illegible to those of us who aren't familiar with technical or legal jargon, but are often written

[108] Alex Argüelles (2020). "#SalvemosInternet para proteger nuestra democracia." *Derechos Digitales*. Available at: https://www.mnemozine.xyz/blog/salvemosinternet-para-proteger-nuestra-democracia.

behind closed doors and rapidly approved without a public comment period. These political tensions between the interests of civil society and those of private companies or industries—which often participate in commercial exchanges with the government, a lucrative business that can lead to acts of corruption that are unfortunately not new in our context—have given rise to unfair practices that restrict or actively ignore the participation of civil society in decision-making, shaping the "set of criteria that establish the limits of the relationships in which we participate" and that constitute the system of "justice" that governs us.

While Internet access and access to technologies—particularly Information and Communications Technologies (ICTs)—can be key to expanding the exercise of our rights, it's clear that, if their implementation doesn't center people's welfare and dignity, then these technologies—and the policies that promote their use—will end up being instrumentalized to consolidate power or perpetuate abuses that can be masked by a discourse of progress and innovation at the expense of the rights of all, but constituting a particular risk to those who have been historically marginalized and excluded from this "progress" for reasons of gender, language, socioeconomic profile or ethnic origins. A clear example of this can be seen in the deepening of the educational divide due to the quarantine measures taken in response to the COVID-19 pandemic, in which

the Public Education Secretariat (SEP) suspended in-person classes in favor of digital programs.

Students at the Mactumactzá Rural Teachers' College in Chiapas denounced this measure because its dependence on technology excluded them from the educational system.[109] On May 18, 2021, they gathered in Chiapa de Corzo to demand respect for their right to education and that they be allowed to take their entrance exams in person, with paper and pen, instead of online: even though Internet access is a right in Mexico, a 2020 study on the availability and use of household information technologies revealed that only 50.4% of the country's rural areas are connected to the Internet. Both the Mactumactzá Rural Teachers' College and its students make up that other half of the population without Internet access, those who could not take advantage of the technosolutionist programs implemented by the SEP—which, besides the cost of connectivity itself, also required having a functional, affordable device in order to take advantage of it.

In response to these demands expressed through legitimate protest, the state deployed a militarized police force to arbitrarily arrest 95 students from rural and Indigenous communi-

[109] Alex Argüelles (2021). "Mactumactzá: derecho a la educación, acceso a internet y violencia estatal." *Animal Político*. Available at: https://www.animalpolitico.com/blog-invitado/mactumactza-derecho-a-la-educacion-acceso-a-internet-y-violencia-estatal/.

ties. On May 24, 74 of these students were freed, denouncing abuse of authority, excessive use of force and sexual violence. Their relatives, as well as those of the students who remained in jail, continued to receive violence from the state—resulting in lesions and gas burns, even among minors and senior citizens—until early June, when the rest were freed.

To date, there's still no information available on the measures that the local government will take to repair the harm done and ensure the rights of the approximately 480 students at the Mactumactzá Rural Teachers' College, who, according to the anthropologist and activist Abel Barrera Hernández, largely belong to the Tzeltal, Tzotzil, Tojolabal, Zoque, Chol and Mam peoples. In response to the May 18 protest, it was announced that the exam would be held in-person on June 9 through devices connected to the Internet that would be provided by the local government, imposing the use of these technologies—despite the specific demand for paper and pens—under the pretext of sanitary measures.

Although we can assume that the Public Education Secretariat's intentions were noble and largely practical, it's simply unacceptable that a federal agency promote measures that are so short-sighted and simplistic, without reflecting on how they could aggravate divides in the exercise of rights among people who live in conditions that are very different than the ones found in the country's major urban areas. Neverthe-

less, the phenomenon of using technologies as definitive, one-size-fits-all solutions is not limited to the educational sector, but has also spread to the cultural, labor, economic, health and public safety sectors as well.

Thinking about technologies in such an arbitrary fashion reveals an ignorance of them, condemning us to live in a society in which we are denied informed participation—and consent—regarding the technologies that are being used to shape the future we'll live in. Technologies aren't solutions, they're simply tools that can help us find the multidisciplinary, flexible solutions that complex problems and diverse contexts truly deserve. Nevertheless, if technologies are implemented in a short-sighted and totalitarian fashion—without space for discussion, dialogue or even trial periods—there are probably other parties for whom technologies are indispensable instruments, as seen in the consolidation of capacities for control and surveillance across Latin America in recent years.

Furthermore, technologies come wrapped up in their own complexities: they aren't free of conflicts and they're definitely not neutral. It's worth asking ourselves who develops the devices and platforms we use, who's behind the commercial agreements that establish the use of one service over another or even what accessibility options would allow these technologies to be used by people with disabilities or those who only speak Indigenous languages. Returning to the case of

the teachers' college, we would need to know the infrastructure that these technologies require, as well as the impact that their deployment would have on nature, such as their consumption of resources: think of the environmental impact of server farms or discarded devices.

Another serious aspect of the implementation of technosolutionist measures, particularly those deployed under an alleged "security" discourse, has to do with the obstacle that they represent for transparency and accountability. Before turning to the most recent and most sophisticated technologies, in the name of historical memory, I'd like to recall the case of the website 1DMX. In December 2012, following the inauguration of President Enrique Peña Nieto, the brutality of the police and arbitrary arrests of journalists and protestors across the country were widely documented through independent efforts that sought to generate a counterweight to the media blackout established by the major outlets, many of which ended up ceding to government pressure to present biased information or simply refusing to cover state violence. The serious human rights violations were evident. The 1dmx.org website thus became the first open repository documenting these abuses, which the government at the time categorically denied.

One year after the website's creation, it was taken down through a joint effort of the Mexican and U.S. governments. Shortly afterward, there was a lawsuit to force the Interior Secretariat

and the National Security Commission to reveal their role in this incident, but they refused to cooperate with the investigation. It's worth mentioning that the director of the National Security Commission at the time was also in charge of the operation that repressed both the protests and their media coverage on December 1, 2012. Some time later, GoDaddy—the company that hosted the website—admitted that the request had come from the Specialized Technological Response Center, a dependency of the National Security Commission's Federal Police.

Although this was one of the first widely-known cases of Internet censorship by the Mexican state, it was definitely not the last attempt to consolidate mechanisms for this purpose. Internet censorship is much more sophisticated nowadays, as are the discourses that aim to legitimize it. We have seen how censorship has advanced through international trade agreements that have incorporated measures to benefit the intellectual property and global entertainment industries (such as the Digital Millennium Copyright Act, or DMCA), thus weakening our rights, as denounced by the campaign #NiCensuraNiCandados,[110] which opposed the reforms to the Federal Copyright Law and the

[110] Alex Argüelles (2020). "¿Pero qué necesidad? Los derechos humanos NO son moneda de cambio." *Derechos Digitales*. Available at: https://www.mnemozine.xyz/blog/2021/5/13/pero-qu-necesidad-los-derechos-humanos-no-son-moneda-de-cambio.

Federal Criminal Code to put them in line with the Intellectual Property chapter of the United States-Mexico-Canada Agreement (USMCA). The "community standards" of the most popular sociodigital platforms are also used to remove content affiliated with social protest, as well as sexual and reproductive health content that allows us to counteract the effects of the ultraconservative policies that have deprived us of this information for generations.

As these measures involve so many intermediaries, it's difficult for us to clearly and effectively track censorship back to its origins, which facilitates the abuse of these mechanisms through impunity for those who request content to be removed, even when said content is in the public interest. This instrumentalization of technology in a country with such high rates of violence against journalists, activists and human rights defenders constitutes a muzzle on the freedom of expression and an obstacle to information—or justice, as we are unable to find those responsible for this digital censorship.

Something similar occurs with the surveillance and interventions in our telecommunications in this country. As documented in a 2019 report on digital surveillance by Sursiendo, there have been many cases since 2010 in which technologies have been used to spy on journalists, activists and human rights defenders, jeopardizing their privacy. The cases that caused the biggest impact were probably those connected to the

#GobiernoEspía report published by R3D: Red en Defensa de los Derechos Digitales in 2017, which revealed the acquisition and illegal use of spyware by the Mexican authorities. Although these abusive interventions were publicly denounced and condemned by many national and international media outlets, we have learned of other surveillance systems acquired by the Mexican state in recent years, completely ignoring the ongoing demands to stop the illegal use of these technologies. In December 2020, through an investigation carried out by Citizen Lab, it became public knowledge that Mexico was the principal customer of systems developed to exploit cellphone vulnerabilities to intercept calls, text messages and geolocation data. In April 2021, it was revealed that, up through 2018, the Attorney General violated the law by continuing to acquire mass geolocation services and indiscriminately using them without the authorization of a judge. These activities, documented by the Superior Auditor of the Federation, became public knowledge through a report by Zorayda Gallegos published in *El País.*[111] To date, all these illegal activities, which constitute abuses of power

[111] Zorayda Gallegos (2021). "La Fiscalía de México ha contratado en los últimos años programas para el espionaje masivo de teléfonos móviles." *El País*. Available at: https://elpais.com/mexico/2021-04-14/la-fiscalia-de-mexico-ha-contratado-en-los-dos-ultimos-anos-programas-para-el-espionaje-masivo-de-telefonos-moviles.html.

by the state and directly violate the right to privacy, remain unpunished or stuck in long investigations that have failed to provide justice to those who were victims of these interventions.

In February 2021, Madeleine Wattenbarger published a report titled "Donde funcionan las cámaras de vigilancia, pero la justicia no"[112] that—as we have seen with digital espionage systems—reveals how, in Mexico, particularly in Mexico City, we have one of the most sophisticated video surveillance systems in the world, yet it is powerless to prevent crime or ensure justice. The deployment of video surveillance cameras in public space is not new, but they have become more sophisticated, even though their use has been prohibited in many cities around the world because their highly invasive nature has a chilling effect, compromising people's privacy and freedom of transit. In Coahuila, a border state in northern Mexico, video surveillance cameras were installed that incorporated facial recognition systems: a biometric surveillance technology. In November 2020, an investigation published by Quinto Elemento Lab revealed that the internal protocols established by the local prosecutor for adding images to the identification database had been rejected to respond to a

[112] Madeleine Wattenbarger (2021). "Donde funcionan las cámaras de vigilancia pero la justicia no." *Rest of World*. Available at: https://restofworld.org/2021/donde-funcionan-las-camaras-de-vigilancia-pero-la-justicia-no/.

request from the FBI to track down two Americans who had participated in the antiracist protests that followed the murder of George Floyd at the hands of the Minneapolis police. In Mexico, neither the persecution of activists nor the fabrication of evidence to incriminate them are new, much less collaboration with the U.S. government. Mexican facial recognition systems now participate in the persecution of this pair of activists on terrorism allegations.

Mass video and biometric surveillance technologies have been denounced internationally for their negative effects on our rights, but also because they have high rates of false positives that tend to criminalize people belonging to historically marginalized ethnic groups. This discrimination, amplified by technological biases, includes that denounced by members of the trans community, who have also been revictimized by systems that don't recognize their gender identity, even when recognized in official documents. Video and biometric surveillance systems nevertheless continue to be promoted by government agencies and national security officials. Once again, they have completely ignored the concerns of civil society regarding the violence that their use represents for the exercise of human rights and the lack of counterweights or safeguards that would effectively protect us from the abuse of these technologies that are not only highly invasive, but completely useless—as exposed by Madeleine's reporting—for ensuring that justice is done.

The attempt to consolidate databases for biometric identification technologies doesn't end there. In December 2020, the Chamber of Deputies approved the General Population Law, which aims to guarantee the right to one's identity through a digital document that would be issued by the Interior Secretariat. While it would not substitute other identification documents, it would allow for the consolidation of yet another highly sensitive database in the hands of the state, as this identity document would incorporate biometric data. When we speak of biometric data, we're referring to facial characteristics, iris scans, fingerprints or even voice records, but really any data on our bodies that can be collected to identify us.

Some of the concerns have to do with the false sense of justice offered by this proposal, which is advertised as a measure to "guarantee the right to one's identity," but the use of technologies, no matter how sophisticated or innovative they may be, does not truly reflect a commitment by the state to recognize the identities of Indigenous populations and—remembering what happened at the Mactumactzá Rural Teachers' College—it's potentially superfluous to say that this measure could instead deepen divides in access to justice, or in this case, to one's identity. This could end up creating even more obstacles to the recognition of the rights of these populations. There's also a great deal of distrust of the consolidation of sensitive data-

bases containing biometric data, as the Mexican government has repeatedly shown that it does not have the capacity to protect databases of personal information, as seen at the National Transparency, Information Access and Personal Data Protection Institute in 2020 or the Mexican Social Security Institute in 2021. In January 2021, Rodrigo Riquelme published a report in *El Economista*[113] listing the 12 most serious known vulnerabilities in databases at public and private institutions across the country, which is something we should keep in mind.

In a similar effort to consolidate biometric databases that could be used for the identification algorithms of surveillance cameras equipped with facial recognition technology, a bill was approved in December 2020 to create a national database of cellphone users, known as PANAUT, with the intention of reducing extortion by phone in Mexico. This initiative echoed RENAUT from 2011, a registry that was ended just one year after its creation when it was shown that it was not only completely useless for reducing extortion rates, but itself gave rise to cases of identity theft as the extortion rate rose by over 40% in 2012, following its implementation. While this initiative is an attempt to "improve security" like many

[113] Rodrigo Riquelme (2021). "2020, en 20 hackeos o incidentes de seguridad en México." *El Economista*. Available at: https://www.eleconomista.com.mx/tecnologia/2020-en-12-hackeos-o-incidentes-de-seguridad-en-Mexico-20210102-0007.html.

other cases we have examined, in the context of the serious economic crisis provoked by the COVID-19 pandemic, it would be completely unnecessary and unjust to spend millions on measures that have already proven to be useless.

The difference between 2011's RENAUT and 2020's PANAUT is that PANAUT incorporates biometric data, although it's not exactly clear what. It's important to mention that, although advertised as a "security" measure, there's no way to participate in an informed fashion without clarity on its implications and—if this measure is approved—we would be denied the possibility of granting or reserving our consent to share our data (including our biometric data), violating our ARCO (Access, Rectification, Cancellation and Opposition) rights. This is aggravated by the fact that this coercive participation determines our right to communication, as—in theory—if we don't participate, our ability to contract a telephone line would be restricted. It's completely naïve to believe that organized crime doesn't have ways around these measures, and even stubborn in light of the RENAUT experience, but it could still—once again—widen the divides that obstruct access to telecommunications and other technologies that can be used as tools to ensure justice.

As with the campaigns #SalvemosInternet, its 2014 predecessor #NoMásPoderAlPoder and #NiCensuraNiCandados, civil society responded to PANAUT with #NoAlPadrón. This campaign

also sought to generate information on the database's implications and raise consciousness on our personal data and the defense of digital rights, offering paths to political participation beyond the most popular sociodigital networks by opening up spaces for dialogue on these issues and generating free writs of protection through the platform https://noalpadron.mx. This is a clear example of how technologies can be used to promote justice through a perspective that convokes diverse sectors to defend our rights.

These varied campaigns, actions and resistances aimed at changing the technological policies that affect our human rights (both positively and negatively) have been promoted through the exercise of our digital rights. We use technologies as tools to share information and digital platforms to convoke others and share resources, communicate with each other and generate a counterweight to the hegemonic narratives of the state.

All these activities, which involve access to information, the freedom of expression, access to culture, access to the Internet, the right to privacy and the protection of our identity and personal data, are also ways in which we construct justice, opening up possibilities to transform the divides, inequalities and authoritarian impositions that threaten our rights.

To take advantage of technologies as tools for ensuring justice, let's return to the questions with which this text began. It's necessary to un-

derstand their scope (and biases) and to situate the way they respond to our needs in a broad sense, encompassing the full complexity of our contexts in order to prevent them from becoming a discriminatory barrier. Here it's important to break with the deceitful notion that technology is a solution. Solutions rooted in social commitment and access to justice cannot be centered on the instrumentalization of tools, they must prioritize dignity and respect for human rights in order to weave these perspectives into creative, local opportunities. This will create environments for innovation and the development of technologies that respond to our specific needs and that are affordable, subject to transparency mechanisms for those who develop and operate them and have the consent and informed participation of the general population.

To paraphrase Phi Requiem, a digital security consultant for human rights defenders: "We use the technologies of the future to resolve the problems of the present with the legislation of the past." The cost that these biases have for the exercise of our rights has been reflected in the autonomy that has slowly been worn down by the implementation of technologies that tend to reinforce inequalities and abuses of power, encouraging the construction of a possible future in which authoritarianism can find an inexhaustible source of control in the tools currently being deployed in our country under a false promise of security.

If we can't participate in the construction of our future, that is also a denial of justice. It's therefore of the utmost importance to encourage participation and advocacy so that, in an informed and organized fashion, we can disrupt the opacity that surrounds these issues and avoid the continued imposition of technosolutionist measures that it will take years to roll back. The terrain of the political is always in dispute. We can't allow these same disputes to keep resurfacing between the same actors, the same powers that have consolidated themselves through the invisibilization and silence they impose in spaces that exclude civil society and our many, varied perspectives. It's important to learn, organize and make an impact to reclaim the opportunity to construct the justice we want for the future, but that is denied to us in the present.

Let's hold on to our memory, let's not forget that technologies are tools and not solutions. Let's learn from existing technologies and let's develop new ones and make them accessible. Let's break with the logics of accelerated progress, let's take the time to imagine and invent a new foundation on which to build the future. Let's build accessible pathways to a justice that transforms our present and opens up futures full of possibilities, no longer bound to a dystopian fate in which we must resign ourselves to the impotence and fear imposed by the authoritarianism that silences consensus and participation. There's still time to act, let's do so together.

**>> THERE'S NO JUSTICE WITHOUT DIVERSE PARTICIPATION.**

**>>>>>>>>>>>>>>>>>>**

**>> THERE'S NO JUSTICE WITHOUT INFORMED CONSENT.**

**>>>>>>>>>>>>>>>>>>**

**>> THERE'S NO JUSTICE WITHOUT ACCESSIBILITY.**

**>>>>>>>>>>>>>>>>>>**

**>> THERE'S NO JUSTICE WITHOUT COUNTERWEIGHTS ON THE POWERS THAT BE.**

**>> THERE’S NO JUSTICE WITHOUT TRANSPARENCY.**

**>>>>>>>>>>>>>>>>>>**

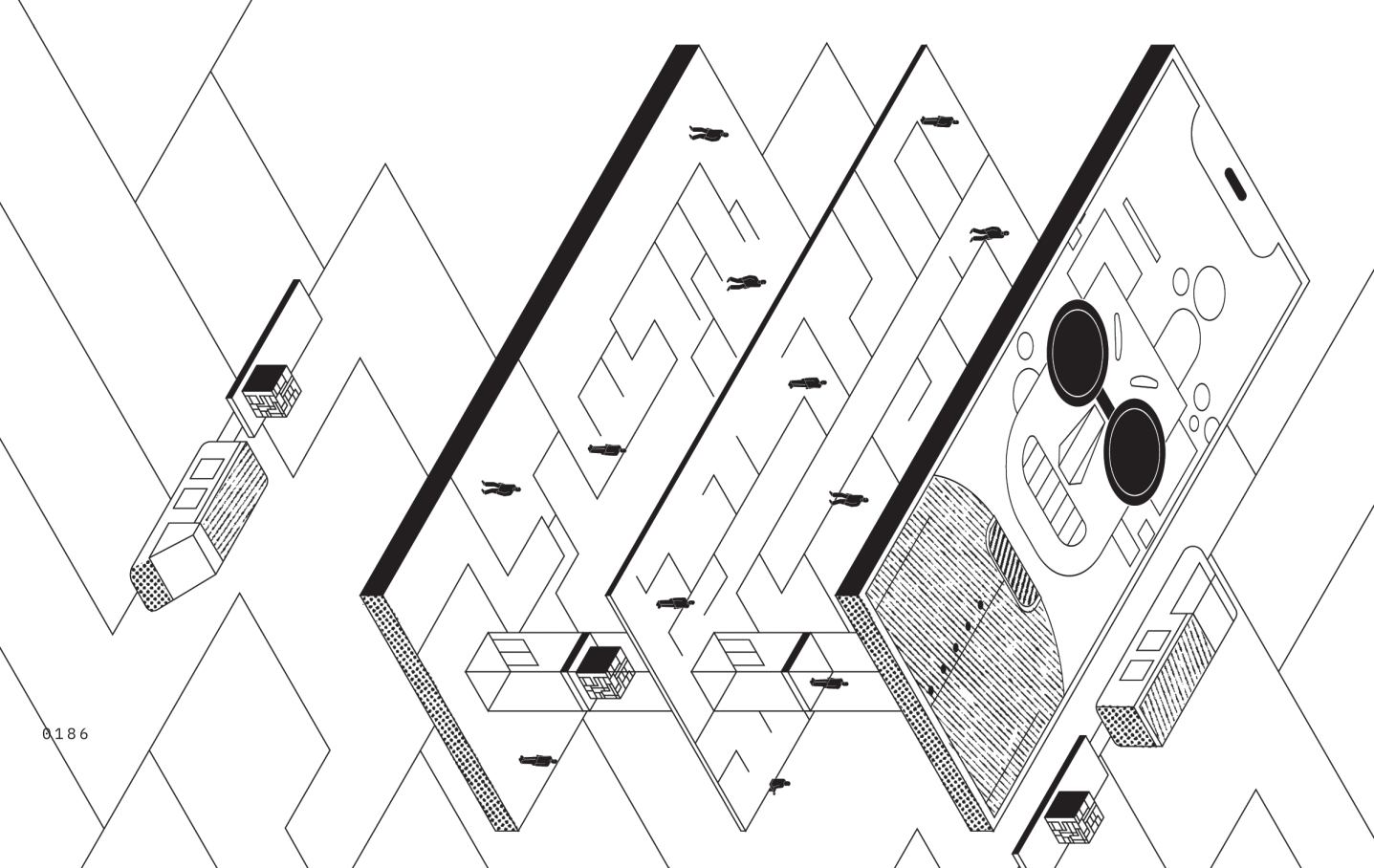
**>> THERE’S NO JUSTICE WITHOUT ACCOUNTABILITY.**

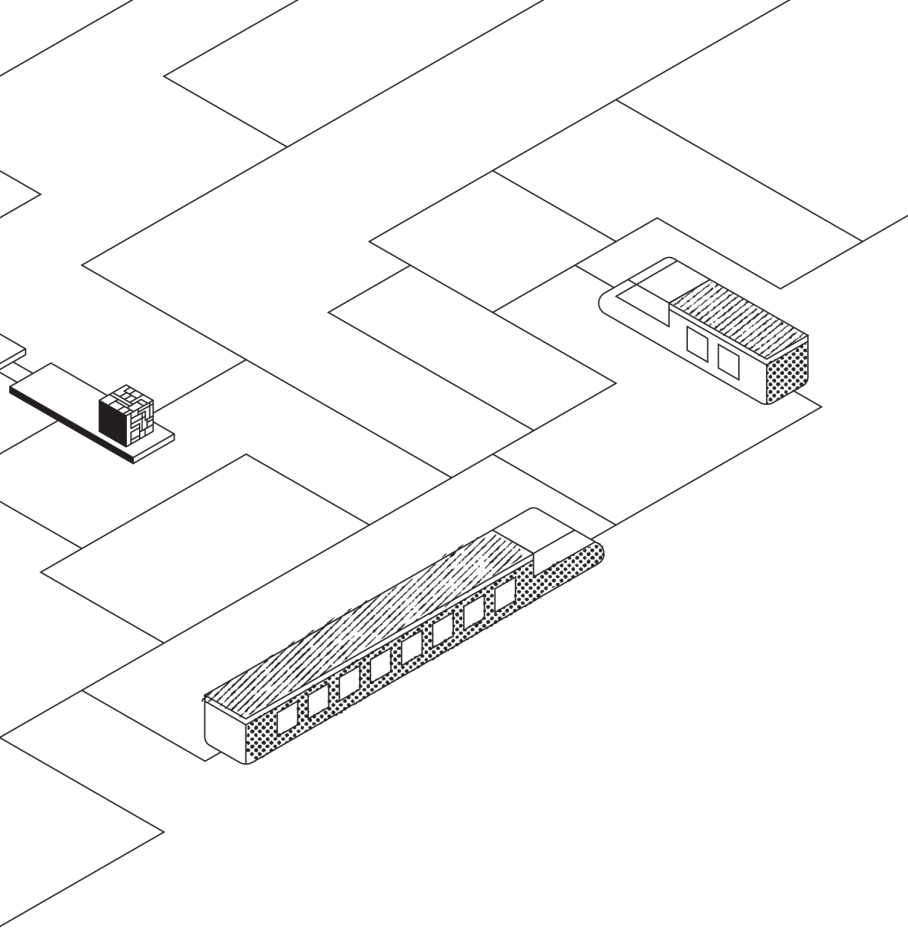
**>>>>>>>>>>>>>>>>>>**

**>> THERE’S NO JUSTICE WITHOUT MEMORY.**

**>>>>>>>>>>>>>>>>>>**

**>> THERE’S NO JUSTICE WITHOUT TRANSFORMATION.**





[This text is an homage]

0188

For more information about digital violence in Mexico, as well as the digital version of this book, information on related events and updated recommendations, visit our website

----------> **https://comun.al**

Let’s learn together!

0189

THIS EDITION WAS PRINTED IN THE WORKSHOPS OF GRUPO ESPINOSA, CENTENO 195, VALLE DEL SUR, 09819, IZTAPALAPA, MEXICO CITY, IN MARCH 2022. THE PRINT RUN WAS 100 COPIES. THE SPANISH EDITION WAS EDITED BY GABRIELA ASTORGA, IVÁN CRUZ OSORIO, BENJAMÍN E. MORALES AND SANTIAGO SOLÍS. FOR THE ENGLISH EDITION, THE TEXT IN SPANISH WAS TRANSLATED AND PROOFREAD BY JULIANNA NEUHOUSER.

THE DESIGN IN BOTH EDITIONS WAS DEVELOPED BY SANTIAGO SOLÍS.

THE FOLLOWING FONTS WERE USED FOR TYPESETTING: LORES 12 OT BY ZUZANA LICKO AND IBM PLEX BY MIKE ABBINK.